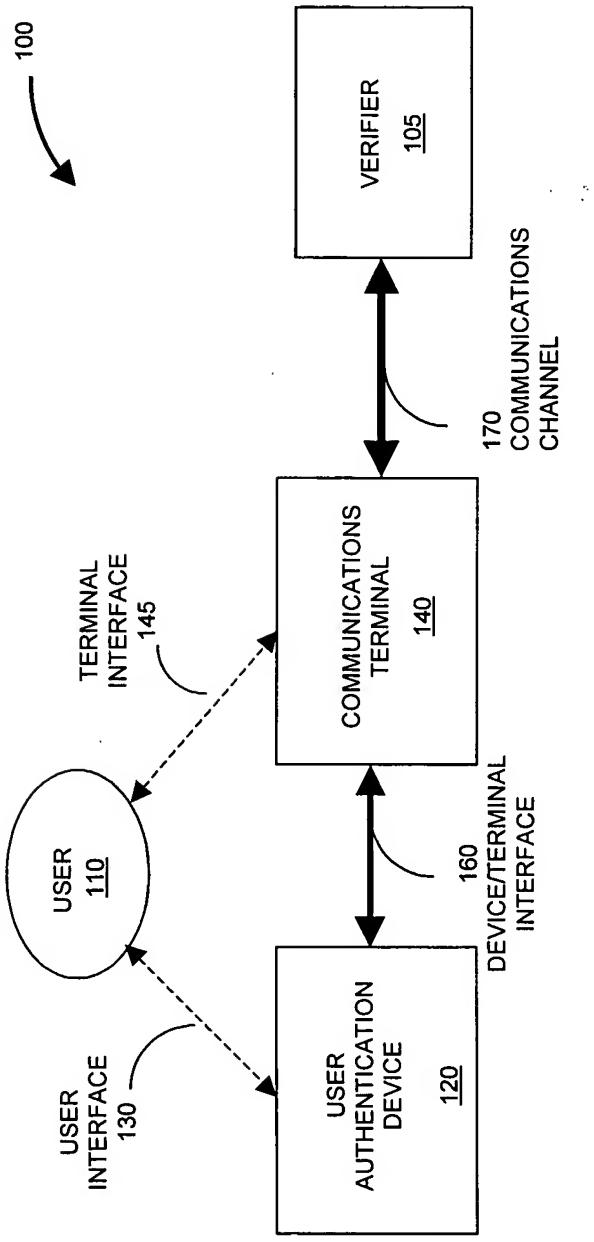
100
VERIFIER
105
170
COMMUNICATIONS
CHANNEL
COMMUNICATIONS
TERMINAL
140
TERMINAL
INTERFACE
145
USER
110
160
DEVICE/TERMINAL
INTERFACE
USER
AUTHENTICATION
DEVICE
120
USER
INTERFACE
130

FIG. 1

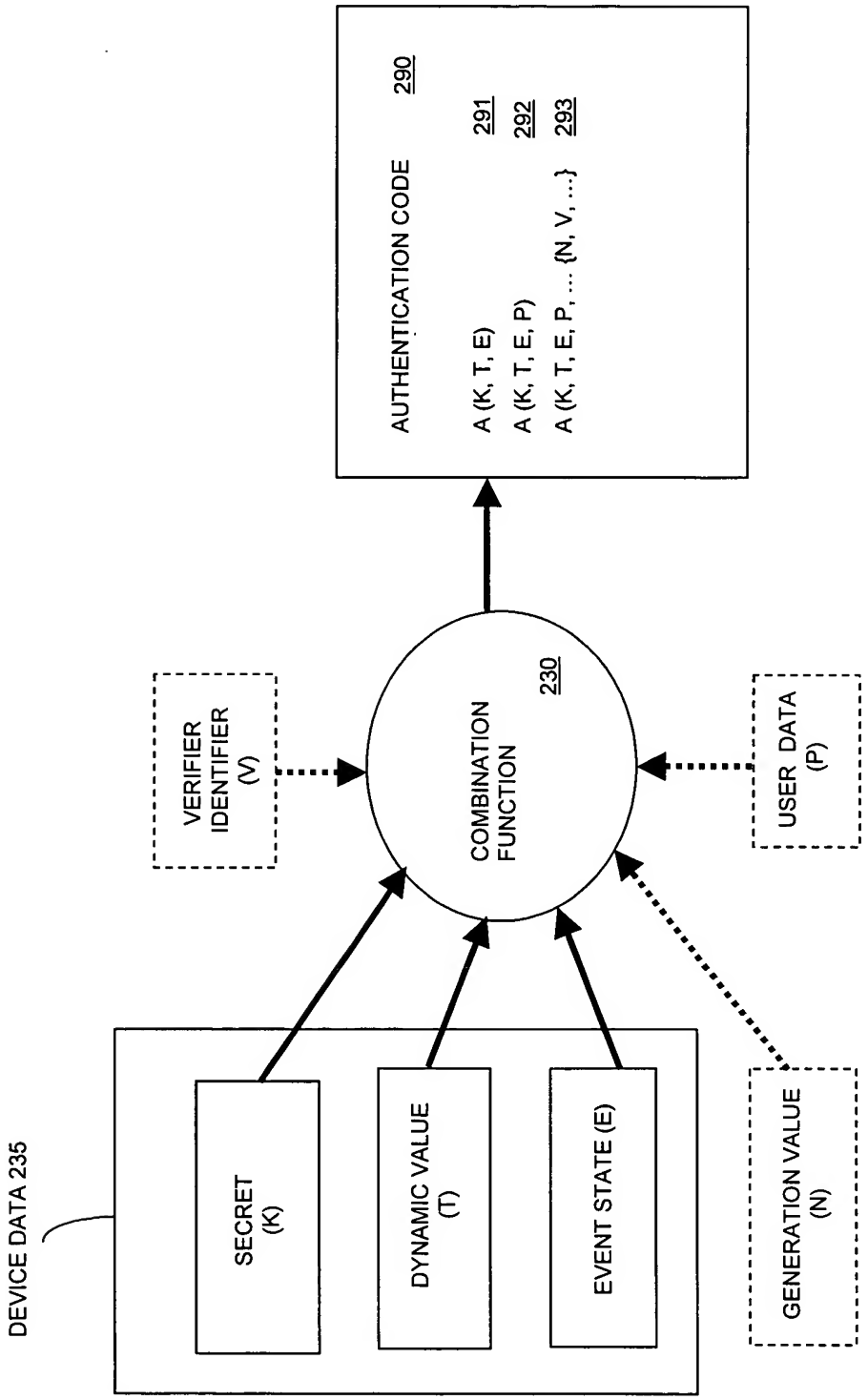
AUTHENTICATION CODE 290
A (K, T, E) 291
A (K, T, E, P) 292
A (K, T, E, P, ... {N, V, ...} 293
COMBINATION FUNCTION 230
VERIFIER IDENTIFIER (V)
USER DATA (P)
DEVICE DATA 235
SECRET (K)
DYNAMIC VALUE (T)
EVENT STATE (E)
GENERATION VALUE (N)

FIG. 2

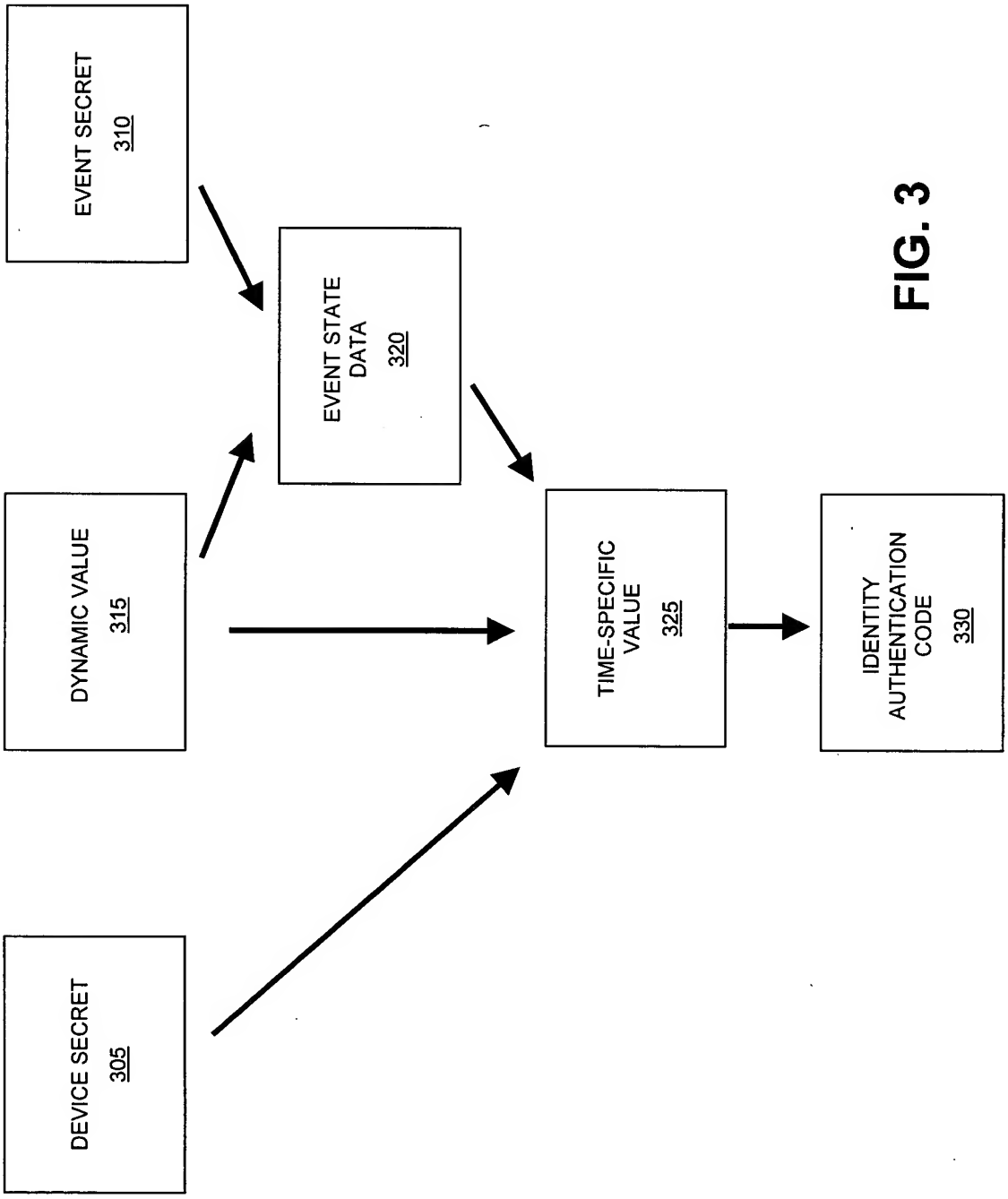
EVENT SECRET
310
EVENT STATE DATA
320
DYNAMIC VALUE
315
TIME-SPECIFIC VALUE
325
IDENTITY AUTHENTICATION CODE
330
DEVICE SECRET
305

FIG. 3

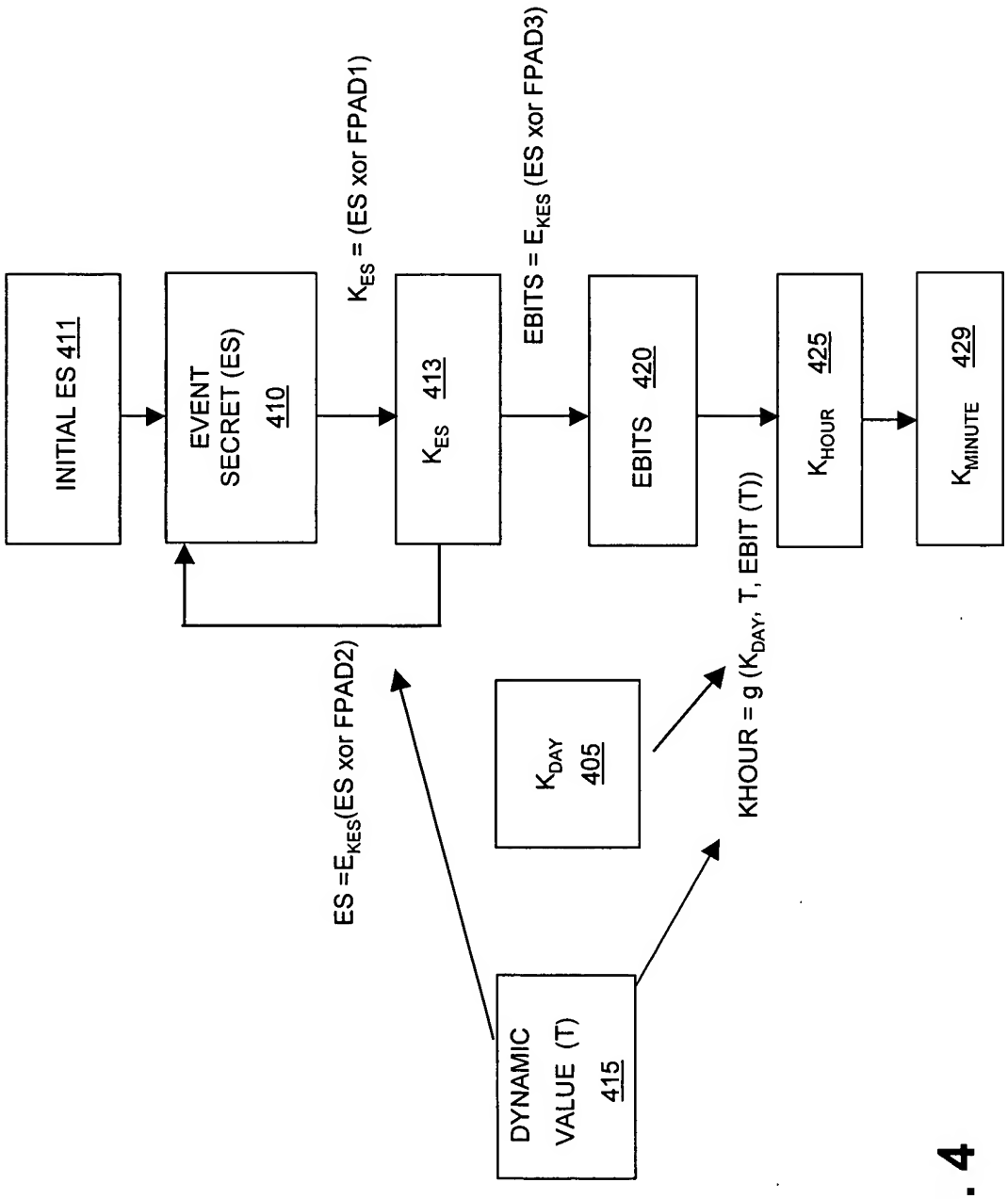
INITIAL ES 411
EVENT SECRET (ES) 410
$K_{ES} = (ES \text{ xor } FPAD1)$
K_{ES} 413
$EBITS = E_{KES} (ES \text{ xor } FPAD3)$
EBITS 420
K_{HOUR} 425
K_{MINUTE} 429
$ES = E_{KES}(ES \text{ xor } FPAD2)$
K_{DAY} 405
$KHOUR = g (K_{DAY}, T, EBIT (T))$
DYNAMIC VALUE (T) 415

FIG. 4

	COLUMN 1 DEVICE SECRET	COLUMN 2 EVENT STATE DATA	COLUMN 3 ACTION	COLUMN 4 OUTPUT
T_1	Initial - A_1	Initial - B_1	-	-
T_2	A_2	B_2	TIME	-
T_3	A_2	B_2	PIN ENTRY	ID AUTH CODE (A_2, B_2)
T_4	A_3	B_3	TIME	-
T_5	A_3	B_4	EVENT REGISTERED	-
T_6	A_4	B_5	TIME	-
T_7	A_4	B_5	PIN ENTRY	ID AUTH CODE (A_4, B_5)

FIG.5

Title: Identity Authentication System and Method
Inventor(s): Jakobsson, et al.
Serial No.: Not Yet Assigned
Atty Docket No.: RSA-061 (7216/119)
Atty/Agent: Robert V. Donahoe
Express Mail Mailing Label No.: EL988703788US
Sheet 5 of 8

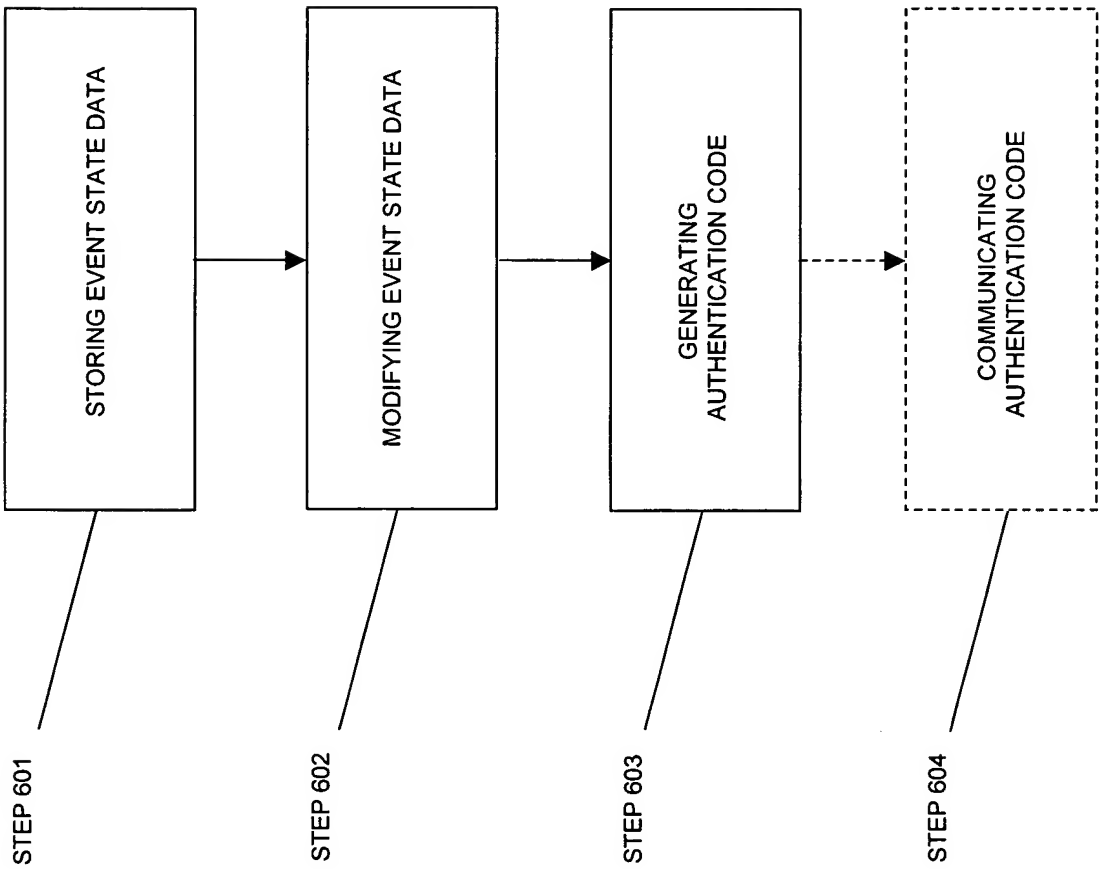
STORING EVENT STATE DATA
MODIFYING EVENT STATE DATA
GENERATING AUTHENTICATION CODE
COMMUNICATING AUTHENTICATION CODE
STEP 601
STEP 602
STEP 603
STEP 604

FIG. 6

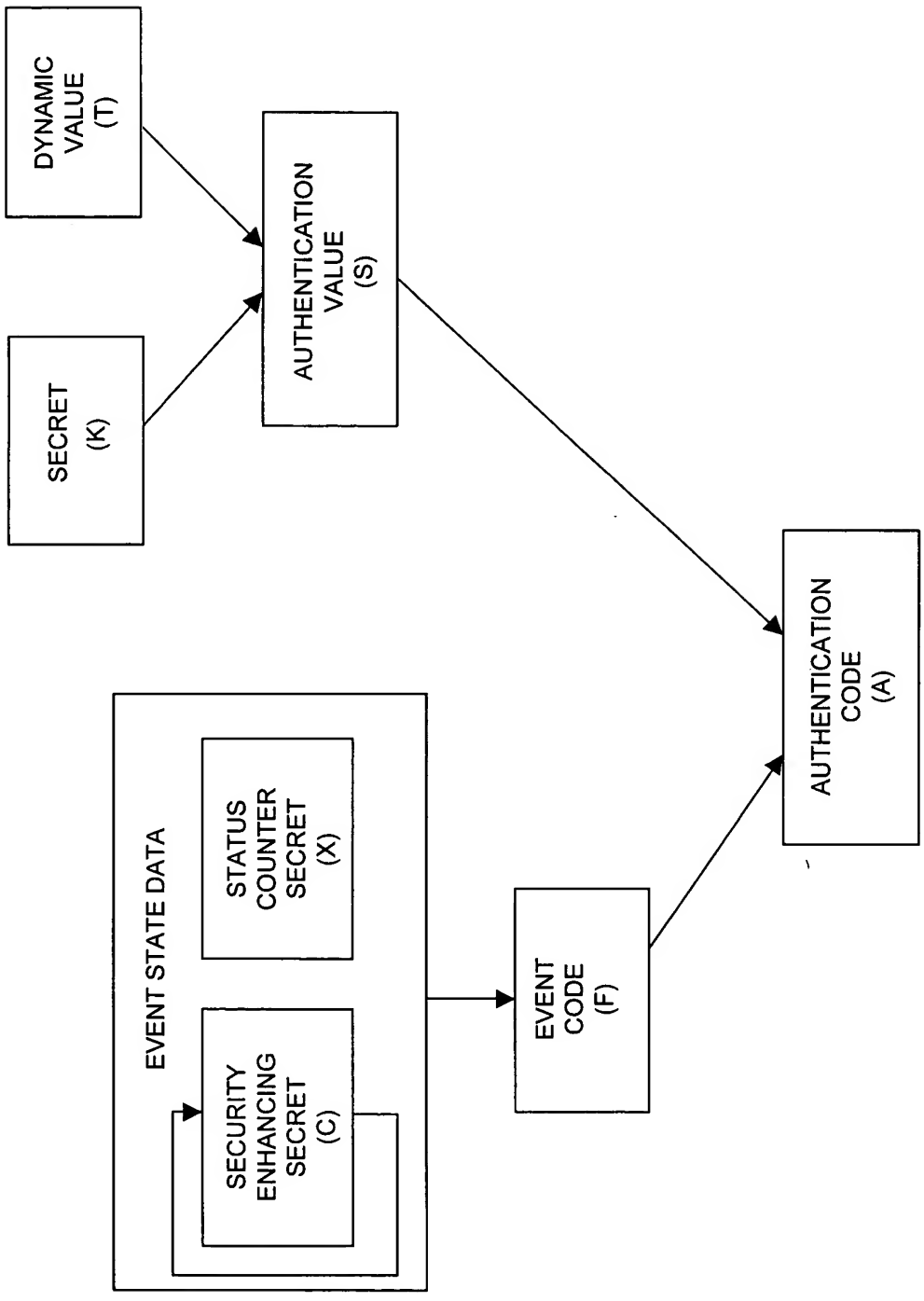
DYNAMIC VALUE (T)
SECRET (K)
AUTHENTICATION VALUE (S)
EVENT STATE DATA
STATUS COUNTER SECRET (X)
SECURITY ENHANCING SECRET (C)
EVENT CODE (F)
AUTHENTICATION CODE (A)

FIG. 7

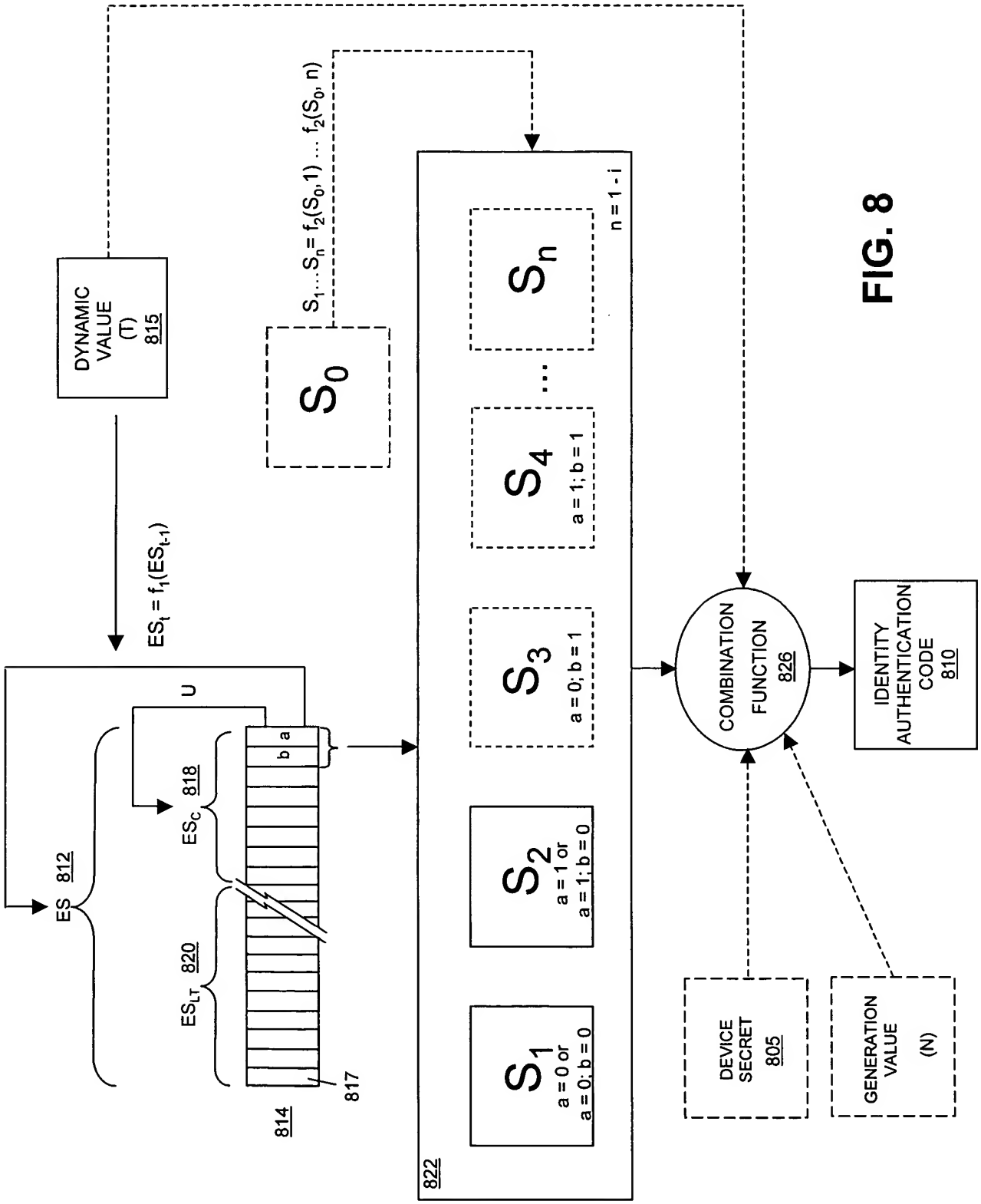
DYNAMIC VALUE (T) 815
$ES_t = f_1(ES_{t-1})$
$S_1 ... S_n = f_2(S_0, 1) ... f_2(S_0, n)$
S_0
S_n
S_4
a = 1; b = 1
S_3
a = 0; b = 1
S_2
a = 1 or
a = 1; b = 0
S_1
a = 0 or
a = 0; b = 0
n = 1 - i
822
U
ES 812
ES_C 818
ES_{LT} 820
b a
814
817
COMBINATION FUNCTION 826
IDENTITY AUTHENTICATION CODE 810
DEVICE SECRET 805
GENERATION VALUE (N)

FIG. 8